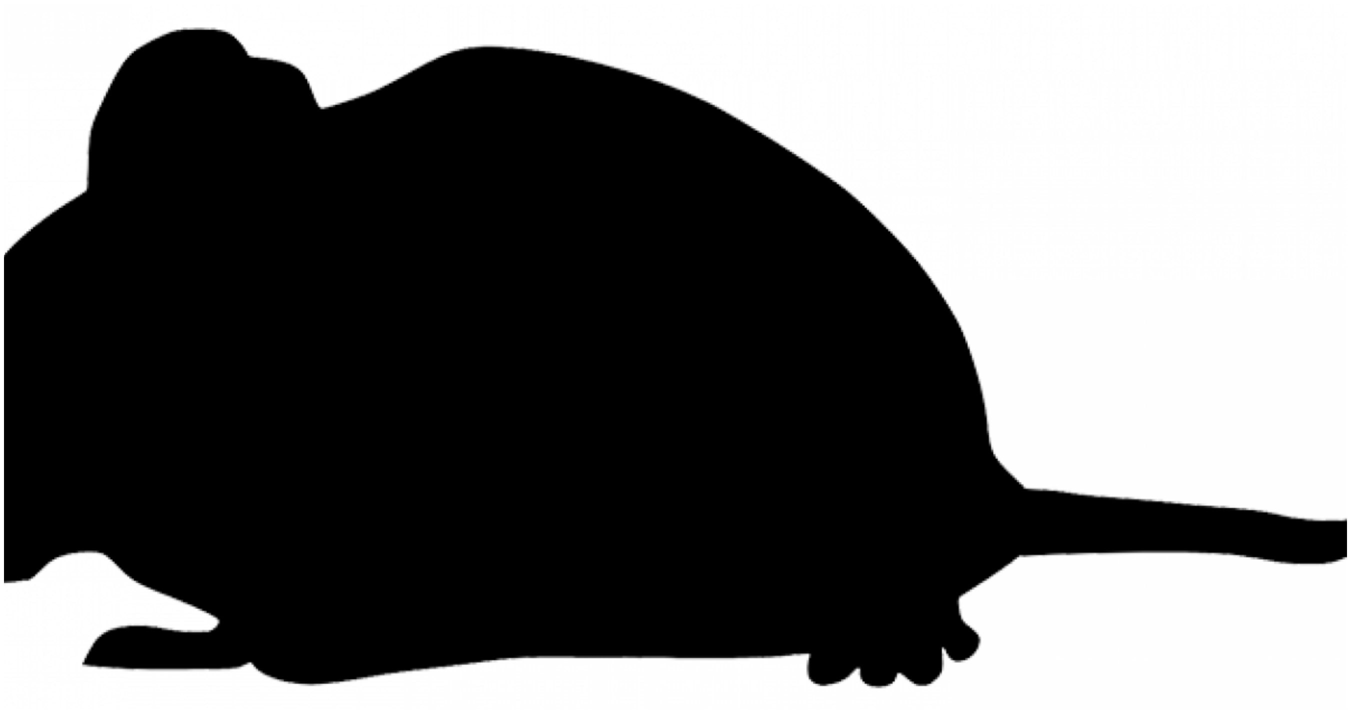
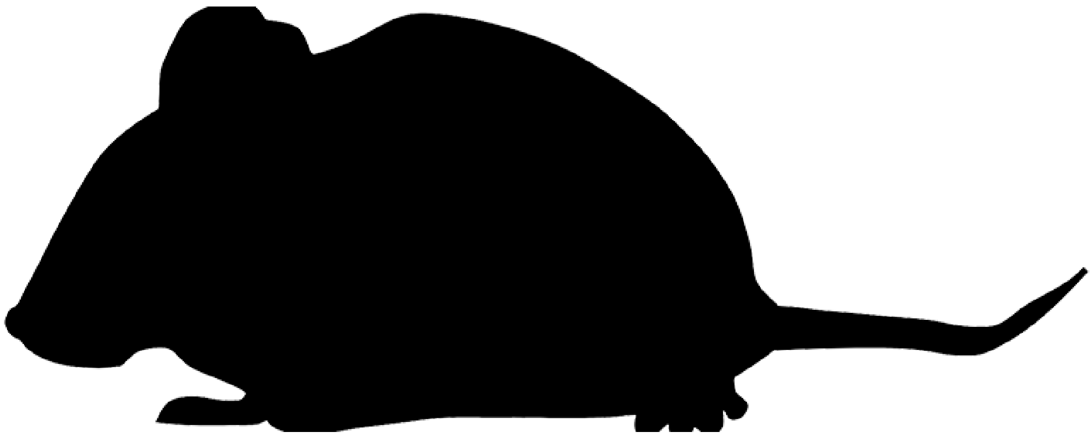
# tRat: New modular RAT appears in multiple email campaigns

proofpoint.com/us/threat-insight/post/trat-new-modular-rat-appears-multiple-email-campaigns

November 15, 2018



tRat: New modular RAT appears in multiple email campaigns



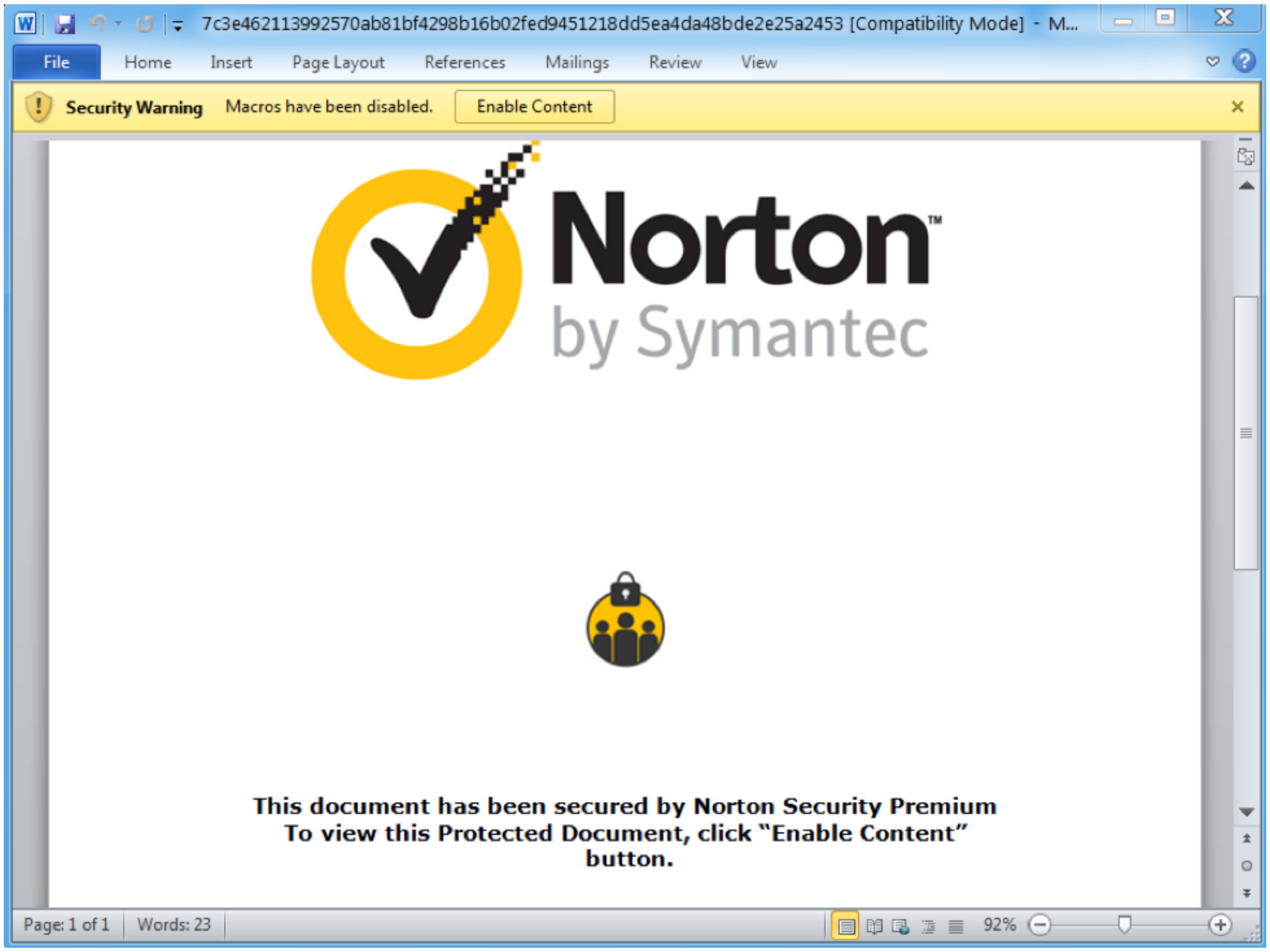
November 15, 2018 Proofpoint Staff

**Overview**

TA505 is one of the most prolific actors Proofpoint tracks. The group was responsible for hundreds of Dridex campaigns beginning in 2014 and massive Locky campaigns in 2016 and 2017, many of which involved hundreds of millions of malicious messages distributed worldwide. More recently, the group has been distributing a variety of remote access Trojans (RATs), among other information gathering, loading, and reconnaissance tools, including a previously undescribed malware we have dubbed tRat. tRat is a modular RAT written in Delphi and has appeared in campaigns in September and October of this year (one of them by TA505). In this blog we discuss the components of these campaigns and provide a brief analysis of the malware.

**Campaigns**

On September 27, 2018, Proofpoint detected an email campaign in which malicious Microsoft Word documents used macros to download a previously undocumented RAT. The documents abused the Norton brand, with the document names and embedded image suggesting that they were protected by a security product. Subject lines on the messages reinforced the social engineering, stating "I have securely shared file(s) with you." Enabling the embedded macros installed tRat. This particular campaign was spread by an unattributed actor, as was an apparently related campaign on September 29 that used a TripAdvisor lure (Figure 2).



This document has been secured by Norton Security Premium
To view this Protected Document, click "Enable Content" button.

*Figure 1: Lure document from campaign on September 27, 2018, using stolen branding and social engineering to trick recipients into enabling malicious macros*

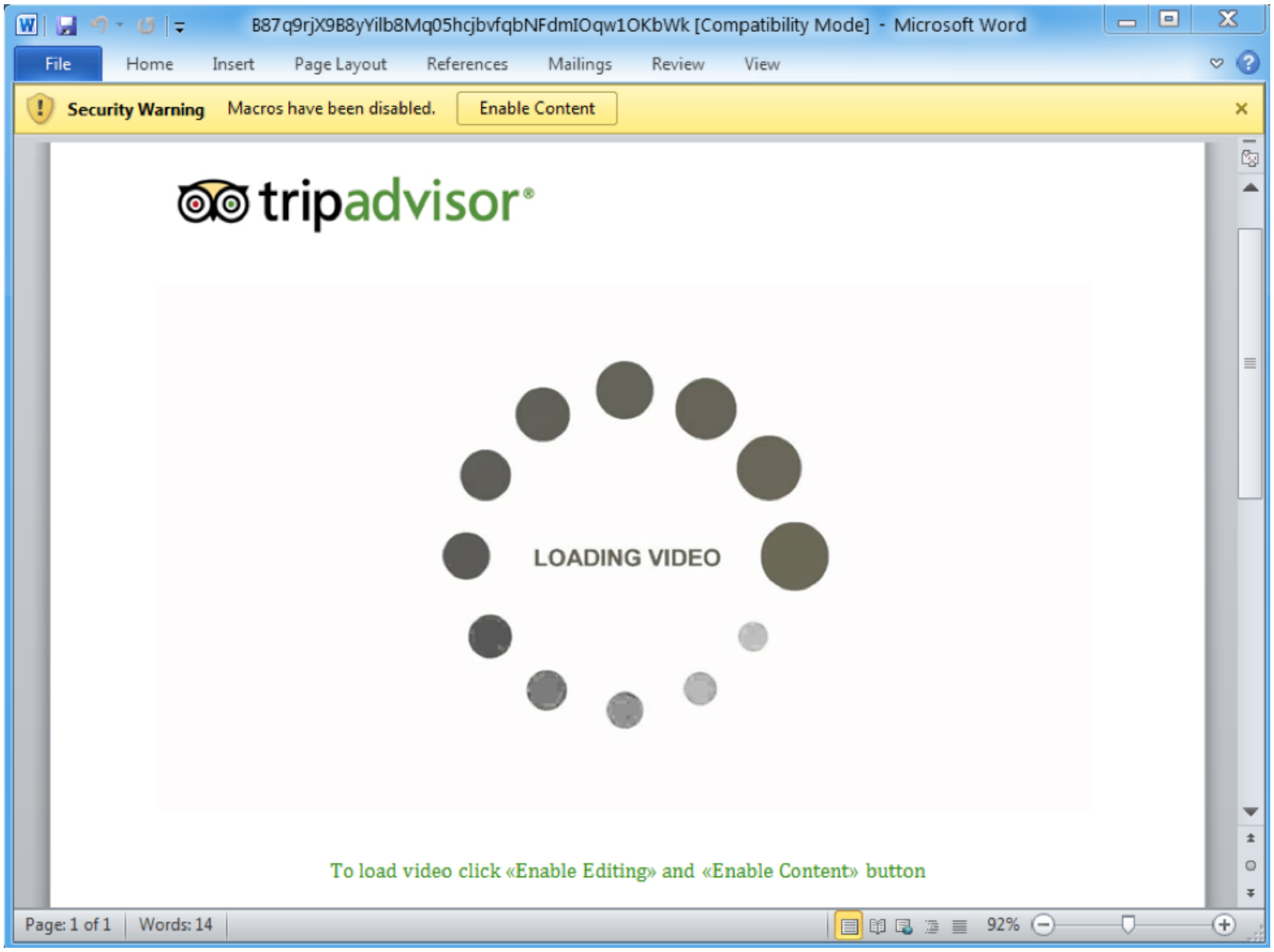
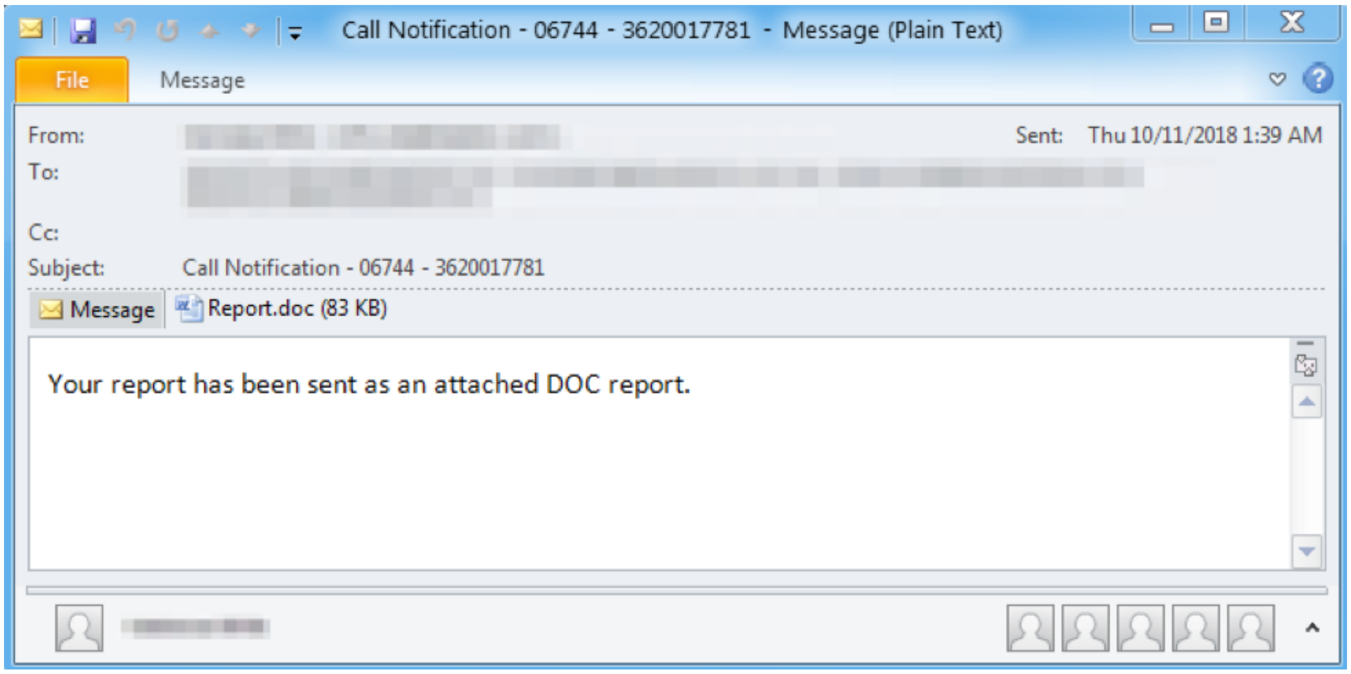

B87q9rjX9B8yYilb8Mq05hcjbvfqbNFdmIOqw1OKbWk [Compatibility Mode] - Microsoft Word
File
Home
Insert
Page Layout
References
Mailings
Review
View
Security Warning
Macros have been disabled.
Enable Content
tripadvisor
LOADING VIDEO
To load video click «Enable Editing» and «Enable Content» button
Page: 1 of 1
Words: 14
92%

*Figure 2: TripAdvisor lure used in a September 29, 2018, campaign, again using stolen branding and social engineering to trick users into enabling macros*

On October 11, we observed another email campaign distributing tRAT, this time by TA505. This campaign was more sophisticated, using both Microsoft Word and Microsoft Publisher files, and varying subject lines and senders. This campaign appeared to target users at commercial banking institutions.

In this campaign, messages bearing malicious Microsoft Publisher documents purported to be from “Invoicing”, with various sending addresses. Example subject lines were "Inovice (sic) [random digits] - [random digits]" and had attachments with names such as "inv-399503-03948.pub". Alternatively, the emails with malicious Microsoft Word attachments appeared to be be from “Vanessa Brito" with various actual sending addresses. Attachments were named “Report.doc” in these messages, with example subject lines such as "Call Notification - [random digits] - [random digits]

Figure 3 shows a sample email:


Call Notification - 06744 - 3620017781 - Message (Plain Text)

From: [redacted]

Sent: Thu 10/11/2018 1:39 AM

To: [redacted]

Cc:

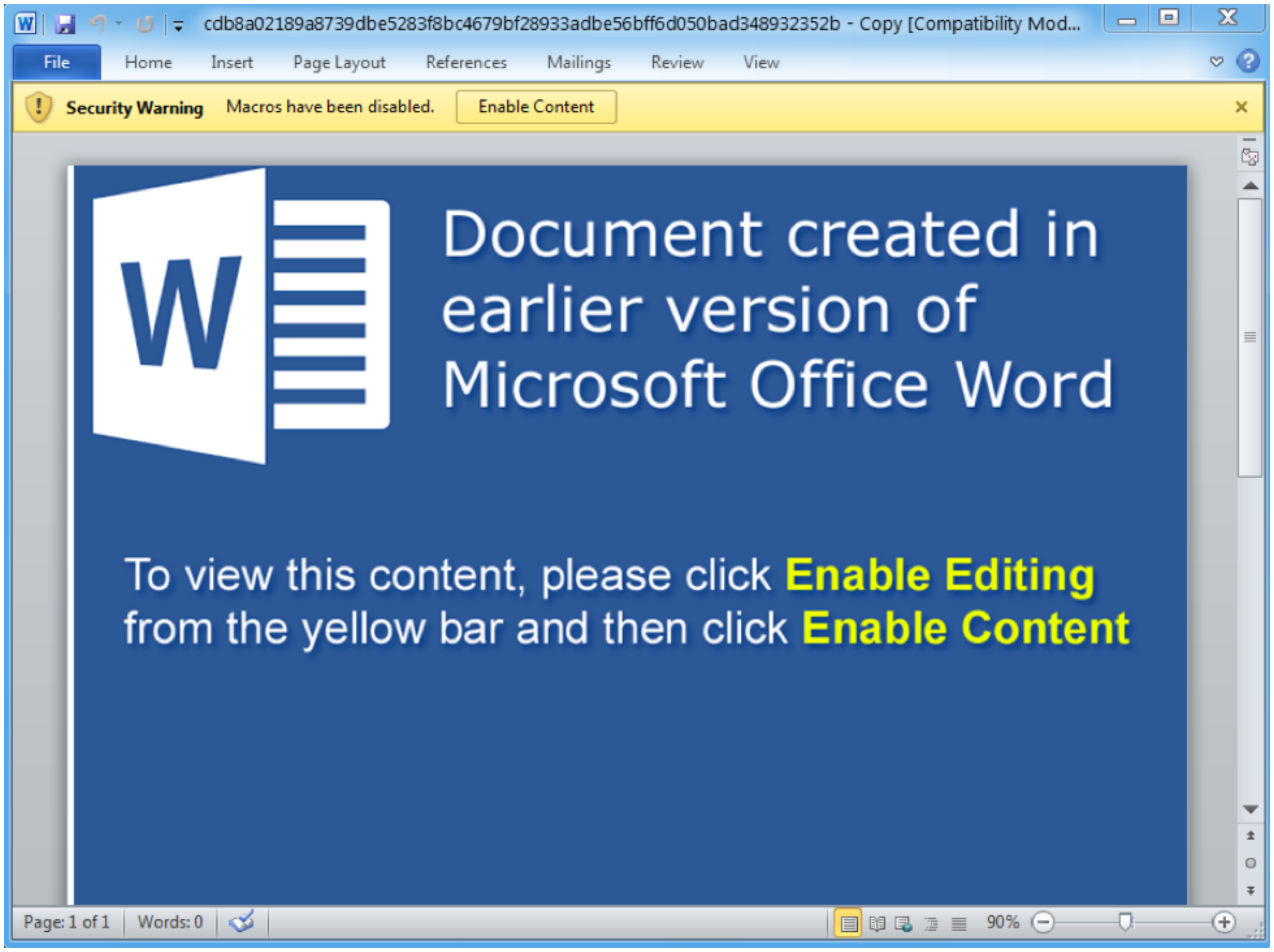
Subject: Call Notification - 06744 - 3620017781

Your report has been sent as an attached DOC report.

[redacted]

*Figure 3: Sample email from campaign on October 11, 2018*

In all cases, the attachments contained macros that, when enabled, downloaded tRat.


cdb8a02189a8739dbe5283f8bc4679bf28933adbe56bff6d050bad348932352b - Copy [Compatibility Mod...

Document created in earlier version of Microsoft Office Word

To view this content, please click **Enable Editing** from the yellow bar and then click **Enable Content**

*Figure 4: Sample lure document from October 11, 2018*

**Analysis**

While we continue to analyze this malware, we have established the functioning of a number of features. In the analyzed sample, tRat achieves persistence by copying the binary to:

C:\Users\<user>\AppData\Roaming\Adobe\Flash Player\Services\Frame Host\fhost.exe

Next, tRat creates a LNK file in the Startup directory that executes the binary on startup:

C:\Users\<user>\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\bfhost.lnk

Most of tRat's important strings are stored encrypted and hex-encoded. A Python script is available [1] on our Github that can be used to decrypt its strings.

tRat uses TCP port 80 for command and control (C&C) communications; data are encrypted and transmitted hex-encoded. To generate the decryption key, tRat concatenates three strings and the result is uppercase hex-encoded. The strings from the analyzed sample are shown below:

1. "Fx@%gJ_2oK"
2. "AC8FFF33D07229BF84E7A429CADC33BFEAE7AC4A87AE33ACEAAC8192A68C55A6"
3. "&LmcF#7R2m"

It is currently unclear whether these strings change from sample to sample. In addition to generating a key, tRat uses a 1536-byte table in the decryption process. As of this writing, we were not able to ascertain the meaning of all elements of the table or determine if it changes. However, we were able to determine that decryption involves XORing various values from the table with the encrypted data. The table indexes are based on the key value, derived as described above. The table [2] from the analyzed sample and a Python script [3] is available on our Github that can be used to decrypt the communications.

tRat's initial phone-home network request is called "AUTH_INF". A decrypted example looks like:

MfB5aV1dybxQNLfg:D29A79D6CD2F47389A66BB5F2891D64C8A87F05AE3E1C6C5CBA4A79AA5ECA29F8E8C8FFCA6A2892B8B6E

This string contains two substrings separated by a ":". The first substring is a hardcoded identifier stored as an encrypted string. The second substring contains encrypted system data as shown below:

FASHYEOHAL/nXAiDQWdGwORzt:3A176D130C266A4D

These data contain the computer name of the infected host, the system username and the tRat bot ID, although we have not yet determined how the bot ID is generated.

In response to the AUTH_INF phone-home, the C&C will respond with "[P]" or a command list. If tRat receives "[P]," it sends "[G]" in reply. While this appears to operate like a command poll, the precise format of the command list, commands, and module data are unknown. Currently, we believe that the only supported command in the loader is "MODULE," which contains at least a module name and export name. To receive a module, tRat performs the following sequence of actions:

- Send "[GET_MODULE]"
- If "[WAIT_FOR_AUTH_INF]" is received, send AUTH_INF data
- If "[WAIT_FOR_MODULE_NAME]" is received, send module name
- The response could be one of the following:
    - "[ERR_MODULE_NOT_FOUND]"
    - "[ACCESS_DENIED]"
    - Module length
- If module length is received, send a "[READY]"
- Receive module
- The module itself is encrypted similarly to the C&C communications, but appears to use different keys that are sent with the module
- Once decrypted, the modules are loaded as a DLL and executed using the received export name

Currently we have not observed any modules delivered by a C&C, so we are unsure of what functionality they might add.

**Conclusion**

TA505, because of the volume, frequency, and sophistication of their campaigns, tends to move the needle on the email threat landscape. It is not unusual for the group to test new malware and never return to distributing it as they have with BackNet, Cobalt Strike, Marap, Dreamsmasher, and even Bart during their ransomware campaigns. However, we observe these new strains carefully as they have also adopted new malware like Locky or less widely distributed malware like FlawedAmmyy at scale following similar tests. Moreover, their adoption of RATs this year mirrors a broader shift towards loaders, stealers, and other malware designed to reside on devices and provide long-term returns on investment to threat actors.

**Indicators of Compromise (IOCs)**

| IOC | IOC Type | Description |
|---|---|---|
| cd0f52f5d56aa933e4c2129416233b52a391b5c6f372c079ed2c6eaca1b96b85 | SHA256 | tRat sample hash, September 27 campaign |
| cdb8a02189a8739dbe5283f8bc4679bf28933adbe56bff6d050bad348932352b | SHA256 | tRat sample hash, October 11 campaign |
| 51.15.70[.]74 | IP | C&C |

**References**

[1] https://github.com/EmergingThreats/threatresearch/blob/master/tRat/decrypt_str.py

[2] https://github.com/EmergingThreats/threatresearch/blob/master/tRat/table

[3] https://github.com/EmergingThreats/threatresearch/blob/master/tRat/decrypt_comms.py

Subscribe to the Proofpoint Blog